Jurnal Elektronik Ilmu Komputer Udayana
Volume 12, No 3. Februari 2024

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Analisis Keamanan pada Aplikasi *Udayana Mobile* Mengacu pada *OWASP Mobile Top 10 2016*

Muhammad Arrysatrya Yusuf Putranda[a1], I Komang Ari Mogi[a2]

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana
Jalan Raya Kampus Unud, Jimbaran, Bali, 80361, Indonesia
[1]yanda4869@gmail.com
[2]arimogi@unud.ac.id

Abstract

Udayana Mobile merupakan aplikasi yang dirilis pada smartphone oleh Universitas Udayana yang bertujuan memudahkan pegawai, dosen, serta mahasiswa mengakses beberapa fitur yang dimiliki Universitas Udayana seperti SIMAK, SIRAISA, SIPENA, dan UKT-Ku. Namun seperti semua aplikasi pada platform smartphone, terdapat kemungkinan isu kerentanan yang ada pada aplikasi Udayana Mobile. Menggunakan MobSF untuk melakukan Analisis Keamanan, dan mengacu pada OWASP *Mobile Top 10 2016.* Didapatkan hasil bahwa aplikasi ini memiliki tiga isu kerentanan. Rincian kerentanan yang ditemukan merupakan *Insufficient Cryptography* (kerentanan akibat kurang kuatnya proses hashing pada aplikasi), *Client Code Quality* (Kerentanan akibat penggunaan database SQLite dimana memungkinan penyerang melakukan serangan SQL Injection), dan *Reverse Engineering* (Kerentanan yang memungkinan penyerang mendapatkan informasi sensitif dari pengguna seperti *username, password, dan key*). Berdasarkan kerentanan tersebut, diberikan rekomendasi dalam peningkatan keamanan aplikasi berupa enkripsi data yang lebih kuat, proses validasi dalam eksekusi *SQL query*, serta teknik obfuscation pada aplikasi.

Keywords: *Udayana Mobile, MobSF, Analisis Keamanan, Owasp Mobile Top 10 2016, Vulnerabillity*

1. Pendahuluan

Perkembangan aplikasi yang berbasis smartphone, terutama android memiliki kemampuan dalam meningkatkan produktivitas seperti tersedianya layanan, fitur serta data yang mudah diakses sehingga banyak digunakan. Saat ini Android menguasai 82,8% pangsa pasar sebagai platform perangkat smartphone di dunia yang paling banyak digunakan [1].

Namun, besarnya pasar Android berbanding lurus dengan besarnya risiko kerentanan yang terdapat pada aplikasi yang tersedia di Android. Menurut laporan *Vulnerabilities and Threats in Mobile Application 2019* yang diterbitkan oleh ptsecurity.com, dilaporkan bahwa aplikasi android memiliki kerentanan yang cukup besar, yakni sebesar 43%. Kerentanan yang umum ditemukan adalah *insecure data storage* yang memiliki presentase sebesar 76%. Kerentanan tersebut sebagian besar disebabkan karena lemahnya keamanan yang dibuat ketika proses pembuatan aplikasi. [2].

Aplikasi berbasis android mulai banyak digunakan di beberapa sektor, salah satunya adalah pada sektor pendidikan. Universitas Udayana merupakan salah satu universitas di Indonesia yang menggunakan teknologi sistem informasi yang memudahkan proses organisasi informasi di kalangan civitas akademik. Salah satunya adalah aplikasi *Udayana Mobile*. Udayana Mobile merupakan aplikasi yang memungkinkan pengguna mengakses beberapa fitur seperti SIRAISA dan SIPENA bagi dosen dan pegawai, serta Sistem Informasi Manajemen Akademik (SIMAK) dan UKT-Ku bagi mahasiswa.

Berdasarkan uraian diatas, penulis melakukan penelitian ini untuk melakukan Analisis Keamanan yang ada pada aplikasi Udayana Mobile dengan menggunakan *OWASP Mobile Top 10 2016* sebagai acuan serta memberikan rekomendasi dari hasil analisis keamanan untuk meningkatkan keamanan pada aplikasi.

2. Metode Penelitian

Metode penelitian yang digunakan pada penelitian ini adalah metode kaulitatif dimana metode ini merupakan metode untuk mengumpulkan data yang berfokus kepada analisis keamanan aplikasi

Udayan Mobile dengan mengacu kepada *OWASP Mobile Top 10 2016* dan menggunakan tools Mobile Security Framework (MobSF).

2.1. Kajian Pustaka

a. OWASP *Mobile Top 10 2016*

Berkembangnya aplikasi berbasis smartphone diiringi dengan tingginya tingkat ancaman serta kerentanan yang ada. OWASP melakukan survei pada tahun 2015 yang bertujuan menganalisis serta mengkategorikan kerentanan yang terdapat pada aplikasi *mobile* yang selanjutnya dirilis sebagai OWASP *Mobile Top 10 2016* dimana ke-10 kerentanan ini berfokus pada aplikasinya, adapun daftarnya adalah [3]:

1. *Improper Platform Usage* [M1]
   Kerentanan ini merupakan kerentanan penyalahgunaan fitur yang ada pada platform serta kegagalan dalam kontrol keamanan yang memungkinkan pengguna mengakses fitur-fitur tertentu meski tidak memiliki akses ke fitur tersebut.

2. *Insecure Data Storage* [M2]
   Kerentanan ini merupakan kerentanan penyimpanan yang tidak aman serta adanya kemungkinan kebocoran data. Kerentanan ini memungkinkan penyerang mengakses berbagai informasi yang disimpan dalam aplikasi seperti informasi pribadi, *cookies* untuk login, dan sebagainya.

3. *Insecure Communication* [M3]
   Kerentanan ini merupakan kerentanan yang umum ditemukan pada aplikasi yang memiliki struktur *client-server* dimana data yang dikirimkan tidak menggunakan enkripsi SSL/TLS.

4. *Insecure Authentication* [M4]
   Kerentanan ini merupakan kerentanan yang terjadi akibat lemahnya prosedur autentikasi serta pengaturan sesi login. Autentikasi pada aplikasi *mobile* dapat bekerja ketika *offline* sehingga dapat diekploitasi oleh penyerang untuk melewati protokol autentikasi.

5. *Insufficient Cryptography* [M5]
   Kerentanan ini merupakan kerentanan akibat lemahnya kriptografi yang lemah serta tidak amannya algoritma kriptografi yang digunakan sehingga penyerang dapat dengan mudah mendekripsikan informasi yang diperoleh.

6. *Insecure Authorization* [M6]
   Kerentanan ini merupakan kerentanan akibat gagalnya suatu server dalam menerapkan identitas serta izin yang benar. Perbedaannya dengan *Inseruce Authentication* adalah jika *Insecure Authentication* mengacu pada pengguna yang mengelabui proses autentikasi, maka *Insecure Authorization* lebih ke kegagalan server pada aplikasi dalam menentukan identitas serta izin.

7. *Client Code Quality* [M7]
   Kerentanan ini merupakan kerentanan akibat kesalahan dalam pembuatan kode aplikasi, dimana hal ini dapat dimanfaatkan untuk melakukan eksploitasi serta berpotensi terjadinya *bypass* kontrol keamanan oleh penyerang.

8. *Code Tampering* [M8]
   Kerentanan in merupakan kerentanan dimana penyerang melakukan modifikasi pada kode aplikasi yang memungkinkan untuk membuat *backdoor* pada aplikasi.

9. *Reverse Engineering* [M9]
   Kerentanan ini merupakan kerentanan yang terkait dengan algoritma enkripsi yang digunakan untuk mencari informasi cara kerja server *back-end*.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

10. *Extraneous Functionality* [M10]
    Kerentanan ini merupakan kerentanan dimana ditemukannya *backdoor* atau bug pada aplikasi yang sengaja dibuat pada saat proses pengembangan namun tidak dihapus ketika masuk produksi sehingga dapat dimanfaatkan penyerang untuk masuk menggunakan *backdoor* tersebut.

b. Mobile Security Framework (MobSF)
Mobile Security Framework atau MobSF merupakan suatu framework yang biasa digunakan untuk melakukan uji penetrasi terhadap aplikasi smartphone secara otomatis, dimana framework ini dapat melakukan pengujian secara statis maupun dinamis serta malware [4]. MobSF dapat digunakan untuk melakukan pengujian keamanan suatu aplikasi binari *Android Package Kit (APK)* dan *iPhone Application (IPA)* serta kode sumber zip. Selain itu MobSF juga dapat melakukan pengujian aplikasi secara dinamis pada saat *runtime* dengan menggunakan metode *fuzzing* [5].

2.2. Analisis Kebutuhan

Kebutuhan Non-Fungsional :

a. Hardware (Perangkat-Keras)
   1. AMD Ryzen 7 4800H
   2. NVIDIA GeForce GTX 1650 Ti
   3. SSD 512GB
   4. RAM 8GB

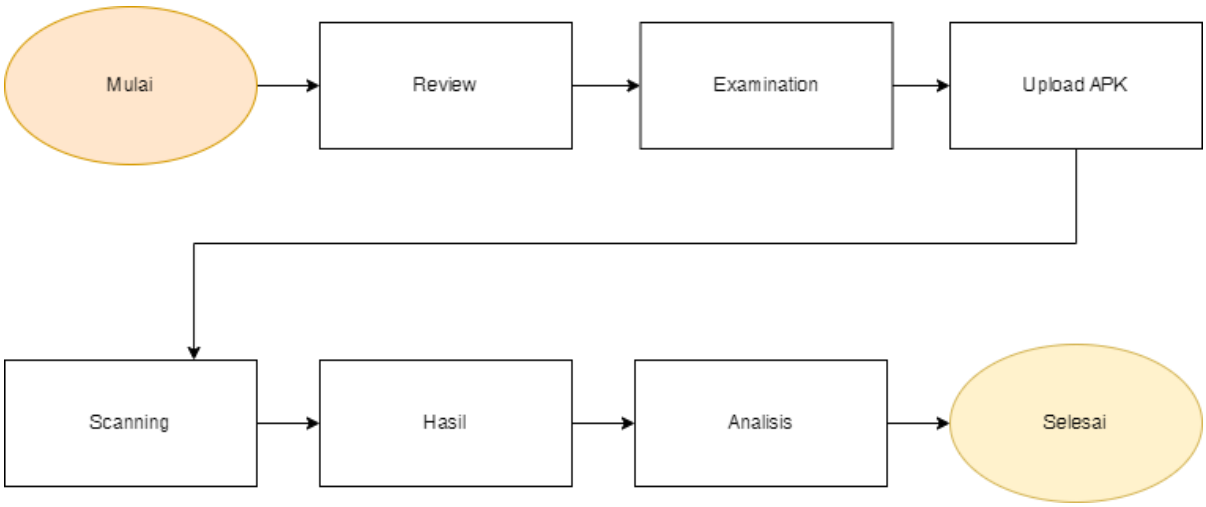
b. Software (Perangkat Lunak)
   1. Windows 10
   2. Mobile Security Framework (MobSF)
   3. Mozilla Firefox
   4. Docker Desktop

Kebutuan Fungsional :

a. Kemampuan meng-ekstraksi file .apk aplikasi
b. Kemampuan menganalisis kerentanan pada aplikasi

2.3. Rancangan Analisis Sistem

Penelitian ini menggunakan metode analisis statik yang dilakukan menggunakan aplikasi Mobile Security Framework (MobSF). Dimana pertama akan dilakukan review mengenai aplikasi seperti izin aplikasi, kemudian berlanjut ke proses examination dimana aplikasi Udayana Mobile akan diupload ke MobSF selanjutnya melalui proses scanning dan hasil scanningnya akan digunakan untuk melakukan analisis kerentanan sesuai dengan OWASP *Mobile Top 10 2016*. Adapun tahapannya dapat dilihat pada **Gambar 1.**



Gambar 1. Flowchart pengujian

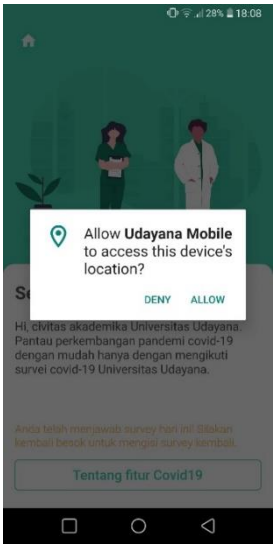
Seperti yang ditampilkan pada **Gambar 1.** Tahapan pengujuan dimulai dari review aplikasi oleh penulis, kemudian berlanjut ke tahap examination dimana aplikasi Udayana Mobile diupload pada MobSF kemudian akan dilakukan proses *scanning*. Setelah proses *scanning* selesai maka hasilnya akan muncul, terakhir akan dilakukan analisis keamanan aplikasi menggunakan hasil *scanning* tersebut dengan mengacu kepada OWASP *Mobile Top 10 2016.*

3. Hasil dan Pembahasan

3.1. Review

Aplikasi Udayana Mobile merupakan aplikasi yang dikembangkan oleh Unit Sumber Daya Informasi Universitas Udayana. Aplikasi ini dapat memudahkan pegawai, dosen, dan mahasiswa mengakses beberapa layanan yang dibutuhkan dalam menunjang kebutuhan akademik di Universitas Udayana seperti SIRAISA dan SIPENA bagi dosen dan pegawai, serta Sistem Informasi Manajemen Akademik (SIMAK) dan UKT-Ku bagi mahasiswa

Gambar 2. Dashboard Udayana Mobile



Gambar 3. Izin akses lokasi

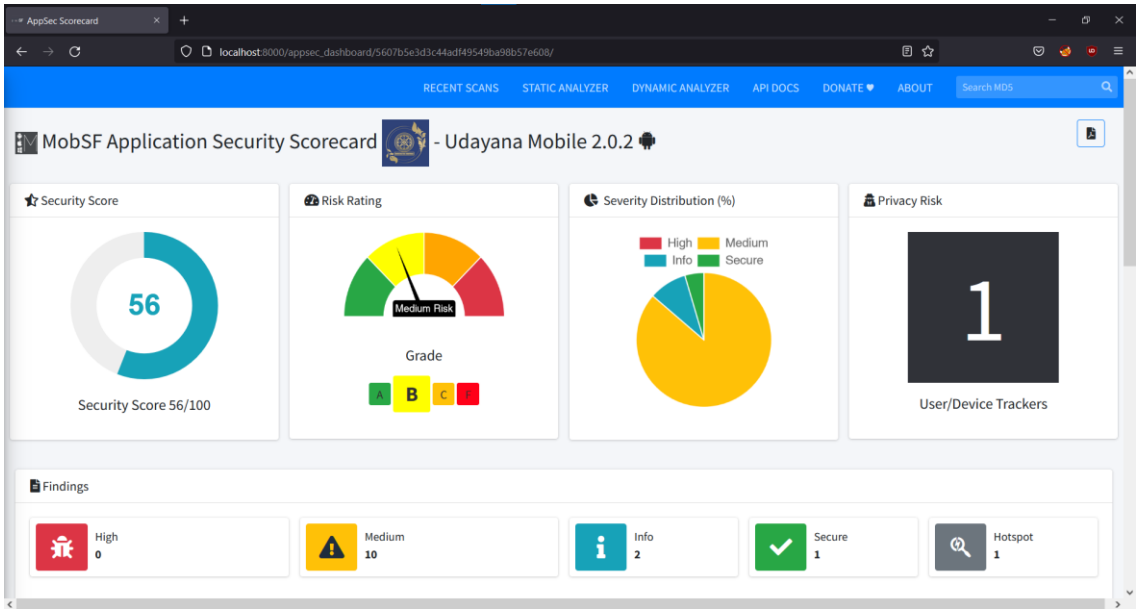
Karena aplikasi ini terintegritas dengan sistem *Integrated Management Information System, the Strategic of UNUD* (IMISSU) milik Universitas Udayana, maka data data pribadi dari pengguna juga disimpan pada aplikasi ini.

Aplikasi Mobile Udayana memiliki izin penggunaan aplikasi, namun tidak langsung meminta izin pengguna ketika diinstall, melainkan permintaan izin muncul ketika mengakses menu tertentu seperti yang ditunjukan pada **Gambar 3.**. Adapun persrtujuan terkait izin untuk lokasi, yakni Izin untuk mengakses lokasi pengguna secara akurat atau perkiraan lokasi.

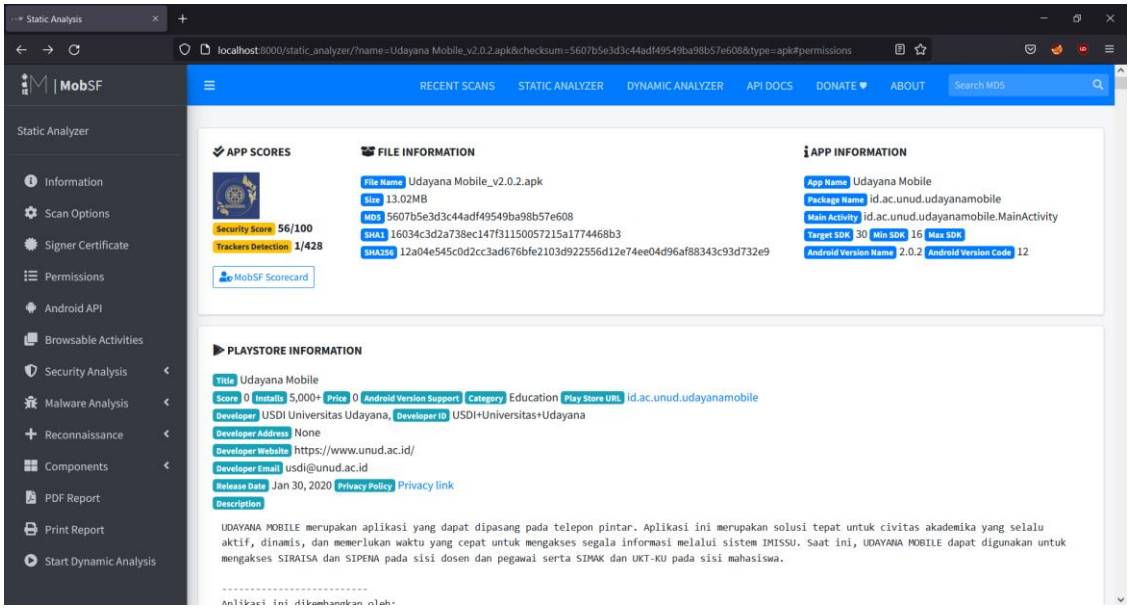
3.2. Examination

Proses *Examination* terdiri dari Upload file APK Udayana Mobile ke MobSF kemudian melalui proses scanning dan hasil dari scanning tersebut akan keluar. Berikut merupakan hasil scanning dari aplikasi Udayana Mobile pada MobSF ditunjukan pada **Gambar 4.** dan **Gambar 5.**

p-ISSN: 2301-5373
e-ISSN: 2654-5101



Gambar 4. Udayana Mobile Scorecard



Gambar 5. Hasil Analisis Aplikasi Udayana Mobile

Tabel 1. Hasil Kerentanan yang Ditemukan

No	OWASP *Mobile Top 10 2016*	Hasil
[M1]	*Improper Platform Usage*	-
[M2]	*Insecure Data Storage*	-
[M3]	*Insecure Communication*	-
[M4]	*Insecure Authentication*	-
[M5]	*Insufficient Cryptography*	√
[M6]	*Insecure Authorization*	-
[M7]	*Client Code Quality*	√
[M8]	*Code Tampering*	-
[M9]	*Reverse Engineering*	√
[M10]	*Extraneous Functionality*	-

3.3. Analisis

Dari **Gambar 1**. Dapat dilihat bahwa aplikasi Udayana Mobile mendapatkan Security Score 56/100 dengan Risk Rating B. Kemudian ditemukan juga 10 *Severity* pada tingkat *Medium.*

Berdasarkan hasil kerentanan yang ditemukan seperti pada **Tabel 1.** Ditemukan 3 jenis kerentanan berdasarkan OWASP *Mobile Top 10 2016* pada aplikasi ini, meliputi :

a. *Insufficient Cryptography* [M5]
Kerentanan ini muncul sebagai peringatan akan adanya kerentanan kriptografi yang terdeteksi pada aplikasi Udayana Mobile. Kerentanan ini berupa penggunaan dari *hascode java* yang digunakan lemah sehingga ada kemungkinan dapat disalahgunakan oleh penyerang.

b. *Client Code Quality* [M7]
Kerentanan ini muncul sebagai peringatan akan adanya isu kerentanan *Cilent Code Quality* dimana aplikasi ini menggunakan database SQLite dan akan mengeksekusi *SQL Query* secara lansung tanpa adanya proses validasi terlebih dahulu. *SQL Query* yang diinput dapat menjadi celah dalam melakukan serangan SQL Injection. Kemudian informasi sensitif pada database tidak dilakukan enkripsi dan hanya disimpan begitu saja pada database.

c. *Reverse Engineering* [M9]
Kerentanan ini muncul sebagai peringatan akan adanya isu kerentanan *Reserve Engineering* dimana ada kemungkinan informasi sensitif seperti *username*, *password*, *keys*, dan lain lain dapat diambil dari aplikasi ini.

4. Kesimpulan

Berdasarkan penelitian ini, dapat disimpulkan Analisis Keamanan pada Aplikasi Udayana Mobile dilakukan secara statis menggunakan MobSF dimana hasilnya aplikasi ini memiliki Security Score yang terbilang cukup, yakni 56/100 dan juga memiliki Risk Rating B. Kemudian terdapat 10 kerentanan pada tingkat medium pada aplikasi ini. Mengacu pada OWASP *Mobile Top 10 2016* ditemukan isu kerentanan pada aplikasi ini diantaranya :

a. *Insufficient Cryptography*
Kerentanan ini merupakan kerentanan akibat lemahnya proses kriptografi yang digunakan pada aplikasi, yakni *java hashcode*. Direkomendasikan untuk melakukan enkripsi ekstra pada sumber kode.

b. *Client Code Quality*
Kerentanan ini muncul akibat penggunaan database SQLite dimana eksekusi query tidak terverifikasi terlebih dahulu sehingga memungkinkan terjadinya serangan SQL Injection. Direkomendasikan melakukan validasi pada query yang dimasukan.

c. *Reverse Engineering*
Kerentanan ini merupakan kerentanan yang cukup berbahaya karena informasi sensitif seperti data login pengguna atau bahkan data pribadi dapat diambil dari aplikasi ini. Direkomendasikan pada sumber kode menggunakan teknik *obfuscation* sehingga ketika terjadi *Reverse Engineering*, *string* yang dihasilkan tidak berupa plain text.

References

[1] N. V. Duc, P. T. Giang, and P. M. Vi, “Permission Analysis for Android Malware,” *Proc. 7th VAST - AIST Work. “RESEARCH Collab. Rev. Perspect.*, no. November 2015, pp. 207–216, 2016.

[2] Candra Kurniawan and N. Trianto, “Security Assessment Pada Aplikasi Mobile Android XYZ Dengan Mengacu Pada Kerentanan OWASP Mobile Top Ten 2016,” *Info Kripto*, vol. 15, no. 1, pp. 11–18, 2021, doi: 10.56706/ik.v15i1.2.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

[3] G. Basatwar, “OWASP Mobile Top 10: A Comprehensive Guide For Mobile Developers To Counter Risks,” *21 September*, 2021. https://www.appsealing.com/owasp-mobile-top-10-a-comprehensive-guide-for-mobile-developers-to-counter-risks/ (accessed Sep. 30, 2022).
[4] F. Nurindahsari and B. Parga Zen, “Analisis Statik Keamanan Aplikasi Video Streaming Berbasis Android Menggunakan Mobile Security Framework (Mobsf),” *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 2, pp. 63–80, 2022, doi: 10.14421/csecurity.2021.4.2.3373.
[5] A. Abraham, Magaofei, M. Dobrushin, and V. Nadal, “Mobile Security Framework MobSF.” https://github.com/MobSF/Mobile-Security-Framework-MobSF.

This page is intentionally left blank.